

In re Patent Application of:
MACCHETTI ET AL.
Serial No. **10/816,791**
Filed: **APRIL 2, 2004**

REMARKS

Applicants would like to thank the Examiner for the thorough examination of the present application. The independent claims have been amended to more clearly define the present invention over the cited prior art references. In particular, independent Claims 12, 17, 23, 28 have been amended to include the subject matter from their respective dependent Claims 13, 20, 24, 31. These dependent claims have been cancelled. Other dependent claims have either been cancelled or amended for consistency. The claim amendments and arguments supporting patentability of the claims are provided below.

I. The Amended Claims

The present invention, as recited in amended independent Claim 12, for example, is directed to a method for generating output bytes corresponding to respective input bytes according to a one-to-one binary function representing a cryptographic algorithm. The method comprises decoding an input byte and generating at least one bit string that contains only one active bit, with the decoding comprising subdividing the input byte into a left nibble and a right nibble, and decoding the left nibble and right nibble into a left 16-bit string and a right 16-bit string, respectively, with each 16-bit string containing only one active bit. The method further comprises using an array of logic gates for logically combining the 16-bit strings according to the one-to-one binary function and generating an encrypted 256-bit string without the use of a lookup table, and encoding the encrypted 256-bit string for obtaining an output byte for the

In re Patent Application of:
MACCHETTI ET AL.
Serial No. 10/816,791
Filed: **APRIL 2, 2004**

cryptographic algorithm.

Amended independent Claim 17 is also directed to a method for generating output bytes, and has been amended similar to amended independent Claim 12, but does not recite the 256-bit string.

Amended independent Claim 23 is directed to a device for implementing a cryptographic algorithm, and has been amended similar to independent Claim 12.

Amended independent Claim 28 is directed to a cryptographic device, and has been amended similar to independent Claim 12.

II. The Amended Claims Are Patentable

The Examiner rejected independent Claims 12, 17, 23 and 28 over the Davida et al. patent. Even though the independent claims were amended to include the subject matter from their respective dependent Claims 13, 20, 24 and 31, the rejection will still be discussed in view of the Davida et al. patent.

The Examiner has taken the position that Davida et al. discloses the claimed invention. As illustrated in FIG. 2 of Davida et al., a substitution box comprises two decoders **1104**, **1105**, each being input with the same n -bit string, and each generating a **decoded** 2^n -bit string (corresponding to the input n -bit string) that contains only one active bit. The device also comprises two encoders **1106**, **1107**, each being input with an encrypted 2^n -bit string generated by re-arranging the bits of the decoded 2^n -bit string according to a respective scheme, and

In re Patent Application of:
MACCHETTI ET AL.
Serial No. **10/816,791**
Filed: **APRIL 2, 2004**

generating corresponding encoded n-bit strings that may contain more than one active bit. A selection circuit **1110** is input with a bit **1113** of a key string for outputting either the encoded n-bit string generated by the first encoder **1106** or generated by the second encoder **1107** depending on the logic value of the bit **1113**.

The Examiner has taken Official Notice that a decoder circuit can be made out of an array of logic gates for logically combining bits of the at least one bit string from smaller sized decoders known as "decode expansion." Along the same lines, the Examiner has taken Official Notice that a decoder circuit can be made from smaller sized decoders in a technique known as "decoder expansion." The Examiner also stated that since it is common and well know in the art that a 2-to-4 decoder is an abstraction of 2 1-to-2 decoders and an array of 4 2-input AND gates, it would have been obvious to extend this to an 8-to-256 decoder by having 2 4-to-16 decoders and an array of 256 2-input AND gates.

The Applicants submit that the Examiner has mischaracterized the Davida et al. patent. The substitution box illustrated in FIG. 2 of Davida et al. is an example of the substitution boxes used in the substitution permutation enciphering and deciphering circuit illustrated in FIG. 1 of Davida et al. As noted above, the substitution box includes encoders **1104**, **1105** and decoders **1106**, **1107** coupled together. Reference is directed to column 5, lines 1-5 of Davida et al., which provides:

In re Patent Application of:

MACCHETTI ET AL.

Serial No. **10/816,791**

Filed: **APRIL 2, 2004**

"It is necessary to connect the decoder outputs to encoder inputs such that the data translation circuit constructed thereby is not only a one to one data translation circuit but is also a complete data translation circuit." (Emphasis added)

As best illustrated in FIG. 2, the outputs of each decoder are connected to different inputs of their respective encoders to provide a one-to-one binary function. The Applicants object to the Examiner taking Official Notice of using smaller sized decoder known as "decode expansion" to provide an array of logic gates for logically combining the 16-bit strings according to the one-to-one binary function and generating an encrypted 256-bit string without the use of a lookup table as in the claimed invention. The Applicants submit there is simply no motivation in Davida et al. to modify the decoders to provide the function of a decoder and an array of logic gates as in the claimed invention.

Moreover, when a "decode expansion" is used for decoding an input byte, the decoded 256-bit string corresponds to the input byte. Consequently, encoding back the decoded 256-bit string would produce an output byte identical to the input byte. This of course defeats the purpose of a substitution box to be in encrypting an output bit string.

In sharp contrast, the left and right decoders and the array of logic gates in the claimed invention do not form an "expanded decoder" of an input byte as purported by the examiner because the structure generates an encrypted 256-bit string and not a decoded 256-bit string. A "decoder expansion" technique would produce a completely different result.

In re Patent Application of:
MACCHETTI ET AL.
Serial No. 10/816,791
Filed: **APRIL 2, 2004**

In the claimed invention, each logic gate in the array of logic gates combines a bit of the left decoded bit-string and a bit of the right decoded bit-string according to a one-to-one binary function for generating an encrypted 256-bit string. This encrypted 256-bit string cannot be obtained merely by decoding the input byte, because the order of the bits is different. Indeed, the one-to-one binary function of the array of logic gates between the left and right decoders and the encoder alters the order of the bits. In other words, when the encrypted 256-bit string is encoded back, an output byte different from the input byte is obtained.

The Applicants also object to the Examiner taking Official Notice that a decoder circuit can be made from smaller sized decoders in a technique known as "decoder expansion" in terms of providing the left and right decoders as recited in the claimed invention. There is simply no motivation to modify the substitution box in FIG. 2 of Davida et al. to produce the claimed invention. Even so, the claimed invention is still not produced since the generated bit string is not encrypted when using the "decoder expansion" technique.

Accordingly, it is submitted that amended independent Claim 12 is patentable over the Davida et al. patent. Amended independent Claims 17, 23 and 28 are similar to amended independent Claim 12. Therefore, it is submitted that these claims are also patentable over the Davida et al. patent.

In view of the patentability of amended independent Claims 12, 17, 23 and 28, it is submitted that their dependent claims, which recite yet further distinguishing features of the


In re Patent Application of:
MACCHETTI ET AL.
Serial No. 10/816,791
Filed: **APRIL 2, 2004**

invention, are also patentable. These dependent claims require no further discussion herein.

III. CONCLUSION

In view of the claim amendments and arguments provided herein, it is submitted that all the claims are patentable. Accordingly, a Notice of Allowance is requested in due course. Should any minor informalities need to be addressed, the Examiner is encouraged to contact the undersigned attorney at the telephone number listed below.

Respectfully submitted,



MICHAEL W. TAYLOR
Reg. No. 43,182
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
407-841-2330